МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

«Юго-Западный государственный университет»

(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«___»_____2017 г.

АНАЛИЗ РАБОТЫ ТЕХНИКИ VLAN

Методические указания по выполнению лабораторной и практической работы по дисциплинам «Сети и системы передачи информации», «Безопасность систем и сетей передачи данных», «Сети и системы передачи информации (специальные разделы)», «Администрирование вычислительных сетей», «Администрирование защищенных телекоммуникационных систем» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00.

Курск 2017

УДК 004
Составители: И.В. Калуцкий, А.Г. Спеваков, Е.В. Шеин, К.О. Хохлач.

Рецензент
Кандидат технических наук, доцент кафедры
«Информационная безопасность» *М.О. Таныгин*

Анализ работы техники VLAN: методические указания к выполнению лабораторных и практических работ по дисциплинам / Юго-Зап. гос. Ун-т; сост. И.В. Калуцкий, А.Г. Спеваков, Е.В. Шеин, К.О. Хохлач. Курск, 2017, 19 с.: ил. 7.; Библиогр.: с. 19.

Содержат сведения по настройке VLAN в среде GNS3. Указывается порядок выполнения лабораторных и практических работ, правила оформления, содержание отчета.

Методические указания по выполнению лабораторных и практических работ по дисциплинам «Безопасность систем и сетей передачи данных», «Сети и системы передачи информации», «Сети и системы передачи информации (специальные разделы)», «Администрирование вычислительных сетей», «Администрирование защищенных телекоммуникационных систем» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00.

Текст печатается в авторской редакции

Подписано в печать Формат 60x84 1/16.
Усл. печ. л. 1,10. Уч. –изд.л. 1,00. Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

VLAN (аббр. от англ. *Virtual Local Area Network*) — логическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – исследовать принцип работы виртуальных локальных сетей VLAN (Virtual Local Area Network) на основе портов и стандарта IEEE 802.1q.

.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Выполнить практическое задание
4. Написать вывод

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Задание в соответствии с вариантом
3. Выполненное задание
4. Вывод

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Виртуальной локальной сетью называется логическая группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса — уникального, группового или широковещательного. В то же время внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с адресом назначения кадра. Таким образом с помощью виртуальных сетей решается проблема распространения широковещательных кадров и вызываемых ими следствий, которые могут развиться в широковещательные штормы и существенно снизить производительность сети.

VLAN обладают следующими преимуществами:

- гибкость внедрения. VLAN являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы, несмотря на их физическое размещение в сети;
- VLAN обеспечивают возможность контроля широковещательных сообщений, что увеличивает полосу пропускания, доступную для пользователя;
- VLAN позволяют повысить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

Типы VLAN:

В коммутаторах могут быть реализованы следующие типы VLAN:

- на основе портов;
- на основе стандарта IEEE 802.1Q;
- на основе стандарта IEEE 802.1ad (Q-in-Q VLAN);
- на основе портов и протоколов IEEE 802.1v;
- на основе MAC-адресов;
- асимметричные.

Также для сегментирования сети на канальном уровне модели OSI в коммутаторах могут использоваться другие функции, например функция *Traffic Segmentation.*

Построение VLAN на основе портов основано только на добавлении дополнительной информации к адресным таблицам коммутатора и не использует возможности встраивания информации о принадлежности к виртуальной сети в передаваемый кадр. Виртуальные локальные сети, построенные на основе стандарта IEEE 802.1Q, используют дополнительные поля кадра для хранения информации о принадлежности к VLAN при его перемещении по сети. С точки зрения удобства и гибкости настроек, VLAN стандарта IEEE 802.1Q является лучшим решением по сравнению с VLAN на основе портов. Его основные преимущества:

1. Гибкость и удобство в настройке и изменении — можно создавать необходимые комбинации VLAN как в пределах одного коммутатора, так и во всей сети, построенной на коммутаторах с поддержкой стандарта IEEE 802.1Q. Способность добавления тегов позволяет информации о VLAN распространяться через множество 802.1Q-совместимых коммутаторов по одному физическому соединению (*магистральному каналу, Trunk Link*);
2. Позволяет активизировать алгоритм связующего дерева (Spanning Tree) на всех портах и работать в обычном режиме. Протокол Spanning Tree оказывается весьма полезным для применения в крупных сетях, построенных на нескольких коммутаторах, и позволяет коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединении портов между собой. Для нормальной работы коммутатора требуется отсутствие замкнутых маршрутов в сети. Эти маршруты могут создаваться администратором специально для образования резервных связей или же возникать случайным образом, что вполне возможно, если сеть имеет многочисленные связи, а кабельная система плохо структурирована или документирована. С помощью протокола Spanning Tree коммутаторы после построения схемы сети блокируют избыточные маршруты. Таким образом, автоматически предотвращается возникновение петель в сети;
3. Способность VLAN IEEE 802.1Q добавлять и извлекать теги из заголовков кадров позволяет использовать в сети коммутаторы и

сетевые устройства, которые не поддерживают стандарт IEEE 802.1Q;

4. Устройства разных производителей, поддерживающие стандарт, могут работать вместе, независимо от какого-либо фирменного решения;
5. Чтобы связать подсети на сетевом уровне, необходим маршрутизатор или коммутатор L3. Однако для более простых случаев, например, для организации доступа к серверу из различных VLAN, маршрутизатор не потребуется. Нужно включить порт коммутатора, к которому подключен сервер, во все подсети, а сетевой адаптер сервера должен поддерживать стандарт IEEE 802.1Q.

ВЫПОЛНЕНИЕ РАБОТЫ

В программе GNS3 постройте следующую топологию:

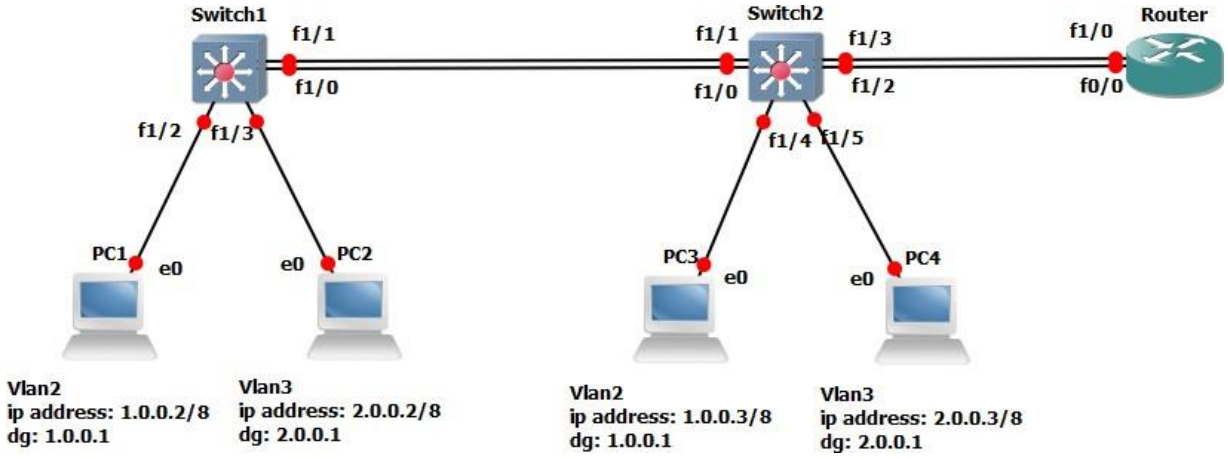

Рисунок 1 – Исследуемая сеть

В данном примере в качестве маршрутизатора используется Cisco 3640 с двумя сетевыми модулями NM-1FE-TX. для моделирования персональных компьютеров используются QEMU или VirtualBox машины с образом операционной системы linux-microcore 2.10 или tinyCore.

Настройка персональных компьютеров

Настройте персональные компьютеры на работу с соответствующими IP адресами. используя следующие команды:

1. Вход в режим суперпользователя:

sudo su

2. Выставить интерфейсу eth0 ip-адрес и маску подсети: ipconfig eth[X] [IP_adress] netmask [MASK]

3. Задать ip-адрес шлюза по умолчанию(default gateway): route add –net 0/0 gw[IP_Gateway]

Пример для компьютера PC1:

tc@box:"$ sudo su

root@box:"# ifconfig eth0 1.0.0.2 netmask 255.0.0.0

root@box:"#route add -net 0/0 gw 1.0.0.1

С помощью следующих команд убедитесь в правильности введенной вами конфигурации:

root@box:"# ifconfig eth0 // для просмотра информации об интерфейсе root@box:"# route // выводит таблицу маршрутизации

После ввода команды route, в таблице должна существовать следующая запись:

Destination Gateway Genmask

Default 1.0.0.1 0.0.0.0

Таким же образом настраиваются оставшиеся персональные компьютеры

Настройка коммутаторов

Перед настройкой коммутаторов составьте таблицу, в которой указано какие номера виртуальных локальных сетей сопоставлены интерфейсам коммутаторов.

Таблица 1 – номера VLAN и связанные с ними интерфейсы

Коммутатор	VLAN2	VLAN3
Switch1	f1/0, f1/2	f1/1, f1/3
Switch2	f1/0, f1/4, f1/2	f1/1, f1/3, f1/5

Настройка коммутатора Switch1

Router>ena
Router#vlan database // команда для входа в режим создания VLAN
Router(vlan)#vlan 2 // создание VLAN 2
VLAN 2 added:

Name:
VLAN0002
Router(vlan)#vlan 3 name QWERTY // создание VLAN 3 с именем
VLAN 3 added: // QWERTY
Name: QWERTY
Router(vlan)#apply // команда применяющая введенные настройки
APPLY completed.
Router(vlan)#exit // команда выхода из режима конфигурации VLAN
APPLY completed.Exiting.... Router#**config t**
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#**hostname SW1**
SW1(config)#**int f1/0**
SW1(config-if)#**switchport access vlan 2** // сопоставление порта f1/0 с VLAN 2
SW1(config-if)#**int f1/1**
SW1(config-if)#switchport access vlan 3 // сопоставление порта f1/1 с VLAN 3
SW1(config-if)#**int f1/2**
SW1(config-if)#switchport access vlan 2 // сопоставление порта f1/2 с VLAN 2
SW1(config-if)#**int f1/3**
SW1(config-if)#switchport access vlan 3 // сопоставление порта f1/3 с VLAN 3

Для просмотра информации о VLAN введите следующую команду SW1#show vlan-switch

VLAN	Name	Status	Ports
1	default	active	Fa1/4, Fa1/5, Fa1/6, Fa1/7 Fa1/8, Fa1/9, Fa1/10, Fa1/11 Fa1/12, Fa1/13, Fa1/14, Fa1/15
2	**VLAN0002**	**active**	**Fa1/0, Fa1/2**
3	**QWERTY**	**active**	**Fa1/1, Fa1/3**
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Рисунок 2 – Информация о VLAN 1

Обратите внимание на выделенные строки.

Для сохранения конфигурации введите следующую

команду:

SW1#copy run start

Destination filename [startup-config]? Y Building

configuration…

[OK]

SW1#

Настройка коммутатора Switch2

Router>ena
Router#vlan
database
Router(vlan)#vlan
2
VLAN 2 added:
Name:
VLAN0002
Router(vlan)#vlan 3
VLAN 3 added:Name: VLAN0003
Router(vlan)#app
ly APPLY
completed.
Router(vlan)#exit
APPLY
completed.
Exiting....
Router#config t
Enter configuration commands, one per line. End
with CNTL/Z. Router(config)#hostname SW2
SW2(config)#int f1/1
SW2(config-if)#switchport
access vlan 3 SW2(config-if)#int
f1/0
SW2(config-if)#switchport
access vlan 2 SW2(config-if)#int
f1/2
SW2(config-if)#switchport

access vlan 2 SW2(config-if)#int
f1/4
SW2(config-if)#switchport
access vlan 2 SW2(config-if)#int
f1/3
SW2(config-if)#switchport
access vlan 3 SW2(config-if)#int
f1/5
SW2(config-if)#switchport
access vlan 3 SW2(config-if)#
*Mar 1 00:03:04.775: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Vlan1, changed state to down
SW2#show vlan-switch brief

VLAN	Name	Status	Ports
1	default	active	Fa1/6, Fa1/7, Fa1/8, Fa1/9 Fa1/10, Fa1/11, Fa1/12, Fa1/13 Fa1/14, Fa1/15
2	VLAN0002	active	Fa1/0, Fa1/2, Fa1/4
3	VLAN0003	active	Fa1/1, Fa1/3, Fa1/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Рисунок 3 – Информация о VLAN 2

После настройки коммутаторов с помощью утилиты Ping проверьте доступность хостов. Компьютеры одной VLAN должны взаимодействовать друг с другом, когда компьютеры из разных VLAN взаимодействовать не будут. Для остановки посылки пакетов нажмите Ctrl+C

Настройка Маршрутизатора

Настройка маршрутизатора тривиальна и состоит в задании соответствующим интерфейсам правильных IP адресов.

Router>ena
Router#config t
Router(config)#int
f0/0
Router(config-if)#ip address 1.0.0.1
255.0.0.0 Router(config-if)#no shutd
Router(config-if)#int f1/0
Router(config-if)#ip address 2.0.0.1
255.0.0.0 Router(config-if)#no shutd

После настройки маршрутизатора снова проверьте доступность хостов с помощью утилиты Ping, если все сделано правильно, то сообщения ICMP эхо запросы должны доходить до любого интерфейса в любой сети.

Составьте следующую топологию

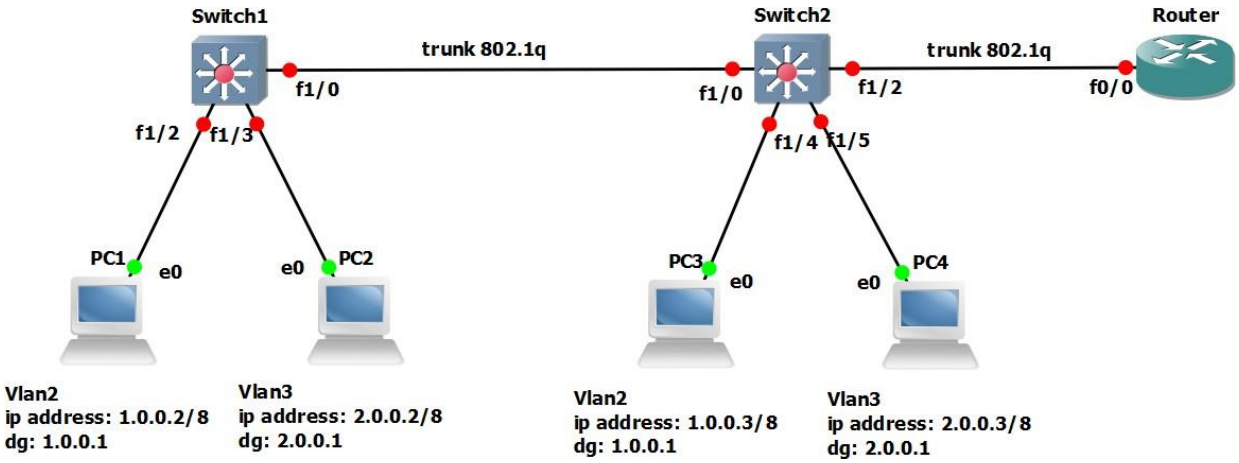

Рисунок 4 – Исследуемая сеть

Настройка компьютеров такая же, как и в предыдущей топологии

Настройка коммутаторов

Настройка коммутаторов полностью идентична, за исключением настройки портов которые стали транкинговыми. Для коммутатора Switch1 это порт f1/0, а для коммутатора Switch2 это порты f1/0и f1/2. В режиме конфигурации этих портов необходимо ввести команду: **switchport mode trunk,** то есть перевести порты в магистральный

режим.

Настройка коммутатора Switch1

Router>ena
Router#vlan
database
Router(vlan)#vlan
2
VLAN 2 added:
  Name:
  VLAN0002
Router(vlan)#vlan 3 name
QWERTY
Router(vlan)#apply
Router(vlan)#exit
Router#config t
Router(config)#hostname
SW1 SW1(config)#int
f1/0
SW1(config-if)#**switchport mode trunk**
SW1(config-if)#int f1/2
SW1(config-if)#switchport
access vlan 2 SW1(config-if)#int
f1/3
SW1(config-if)#switchport
access vlan 3 SW1#show vlan-
switch

После ввода этой команды обратите внимание что порт который стал транкинговым не принадлежит ни одной VLAN

SW1#**show int f1/0 switchport**
Name: Fa1/0
Switchport: Enabled
Administrative Mode:
trunk Operational Mode:
trunk
Administrative Trunking Encapsulation:
dot1q Operational Trunking Encapsulation:

dot1q Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1
(default) Trunking VLANs Enabled:
ALL **Trunking VLANs Active: 1-3**
Priority for untagged frames: 0
Override vlan tag priority:
FALSE Voice VLAN: none
Appliance trust: none

Внимательно посмотрите на выведенную информацию, из которой видно режим работы порта, тип инкапсуляции, и номера VLAN, которые разрешены на транкинговом порте. Сохраните конфигурацию.

SW1#copy run start
Destination filename [startup-config]?
y Building configuration...
[OK]
SW1#

Настройка коммутатора Switch2

Router>ena
Router#vlan
database
Router(vlan)#vlan
2
Router(vlan)#vlan 3
Router(vlan)#apply
Router(vlan)#exit
Router#config t
Router(config)#hostname
SW2 SW2(config-if)#int
f1/0
SW2(config-if)# **switchport mode trunk**
SW2(config-if)#int f1/2
SW2(config-if)# **switchport mode trunk**
SW2(config-if)#int f1/4
SW2(config-if)#switchport
access vlan 2 SW2(config-if)#int
f1/5

SW2(config-if)#switchport
access vlan 3 SW2(config-if)#
SW2#show vlan-switch
brief SW1#show int f1/0
switchport
SW1#show mac-address-table //просмотр таблицы коммутации

Destination Address	Address Type	VLAN	Destination Port
c403.0f04.0000	Self	1	Vlan1
cc05.1674.0000	Dynamic	2	FastEthernet1/0
cc05.1674.0000	Dynamic	3	FastEthernet1/0
00aa.0078.2600	Dynamic	3	FastEthernet1/3
00aa.0018.4f00	Dynamic	2	FastEthernet1/2
00aa.0026.f900	Dynamic	3	FastEthernet1/0
00aa.009a.9400	Dynamic	2	FastEthernet1/0

Рисунок 5 – Просмотр таблицы коммутации

Обратите внимание на столбец VLAN.

После настройки коммутаторов с помощью утилиты Ping проверьте доступность хостов. Компьютеры одной VLAN должны взаимодействовать друг с другом, когда компьютеры из разных VLAN взаимодействовать не будут.

Настройка маршрутизатора

Для работы с VLAN на маршрутизаторе необходимо сконфигурировать столько подинтерфейсов сколько VLAN существует, затем указать тип инкапсуляции для каждого подинтерфейса и задать ip адрес каждому подинтерфейсу маршрутизатора. Перед созданием подинтерфейса необходимо командой no shutdown включить основной интерфейс.

Например, для создания подинтерфейса 43 на интерфейсе f0/0, необходимо в режиме конфигурации ввести interface f0/0.43. Номер интерфейса ни как ни связан с номером VLAN, но для удобства, как правило, номер подинтерфеса устанавливают равным номеру VLAN. то есть интерфейс f0/0.43 может принадлежать VLAN 50 и на оборот, интерфейс f0/0.50 может принадлежать VLAN 43, но одновременно

интерфейс f0/0.43 не может принадлежать сразу двум VLAN

Указание типа инкапсуляции: encapsulation dot1Q [*номер VLAN*]

Пример конфигурации маршрутизатора

Router>ena
Router#config t
Router(config)#int f0/0 // заходим на основной интерфейс
Router(config-if)#no shutdown// включаем его
Router(config-if)#**int f0/0.2** //создаем подинтерфейс номер 2
Router(config-subif)#**encapsulation dot1Q 2** // задаем тип инкапсуляции dot1q, а 2 указывает номер VLAN, к которой принадлежит данный подинтерфейс
Router(config-subif)#ip address 1.0.0.1 255.0.0.0 // устанавливаем ip адрес
Router(config-subif)#exit // выход из режима конфигурации подинтерфейса
Router(config)#**int f0/0.3**
Router(config-subif)#**encapsulation dot1Q 3** Router(config-subif)#ip address 2.0.0.1 255.0.0.0
Router(config-subif)#^Z
Router#show
Router#show ip
route
C 1.0.0.0/8 is directly connected, **FastEthernet0/0.2**
C 2.0.0.0/8 is directly connected, **FastEthernet0/0.3**

Обратите внимание на номера интерфейсов, к которым подключены сети 1.0.0.0 и 2.0.0.0. После настройки маршрутизатора с помощью утилиты ping проверьте связь между компьютерами, находящимися в разных VLAN

Анализ форматов кадров

Во время или до запуска утилиты Ping между хостами PC1 и PC2 запустите сетевой анализатор протокола WireShark и посмотрите перехваченные пакеты между коммутаторами и между хостом и коммутатором, обратите внимание на разные форматы кадров. Точки захвата указаны стрелками на рисунке 6. Для остановки посылки

пакетов ICMP нажмите Ctrl+C

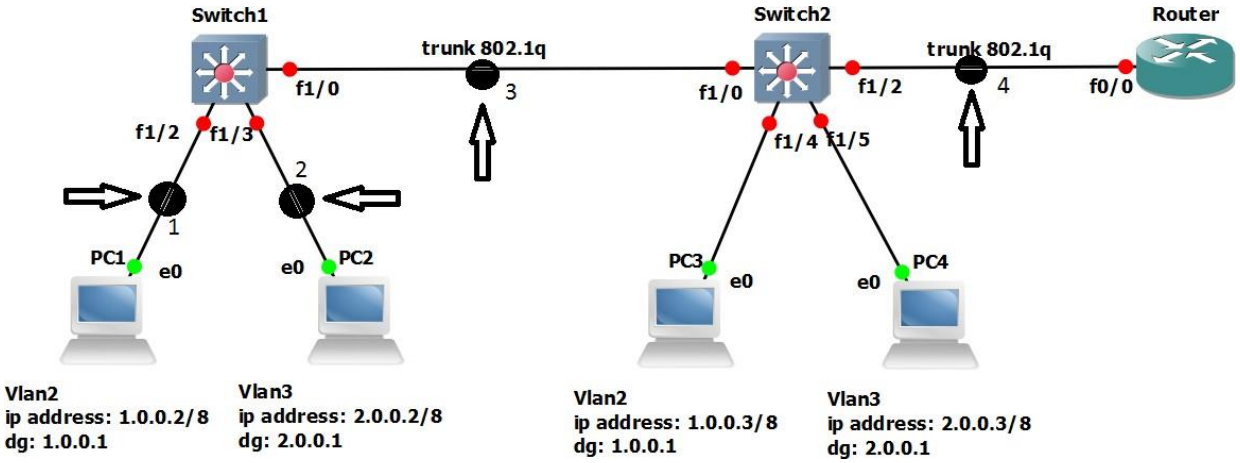

Рисунок 6 – Места захвата пакетов

На рисунке 7 изображено окно сетевого анализатора пакетов, в котором отображен формат пакета ICMP(столбец Protocol, цифра 3) echo request (столбец info, цифра 4) отправленного с адреса 1.0.0.2 (столбец source цифра 1), на адрес 2.0.0.1 (столбец destination, цифра 2). Детализация захваченного пакета показана в окне ниже, а заголовок Ethernet (цифра 5) и заголовок IP (цифра 6) выделены.

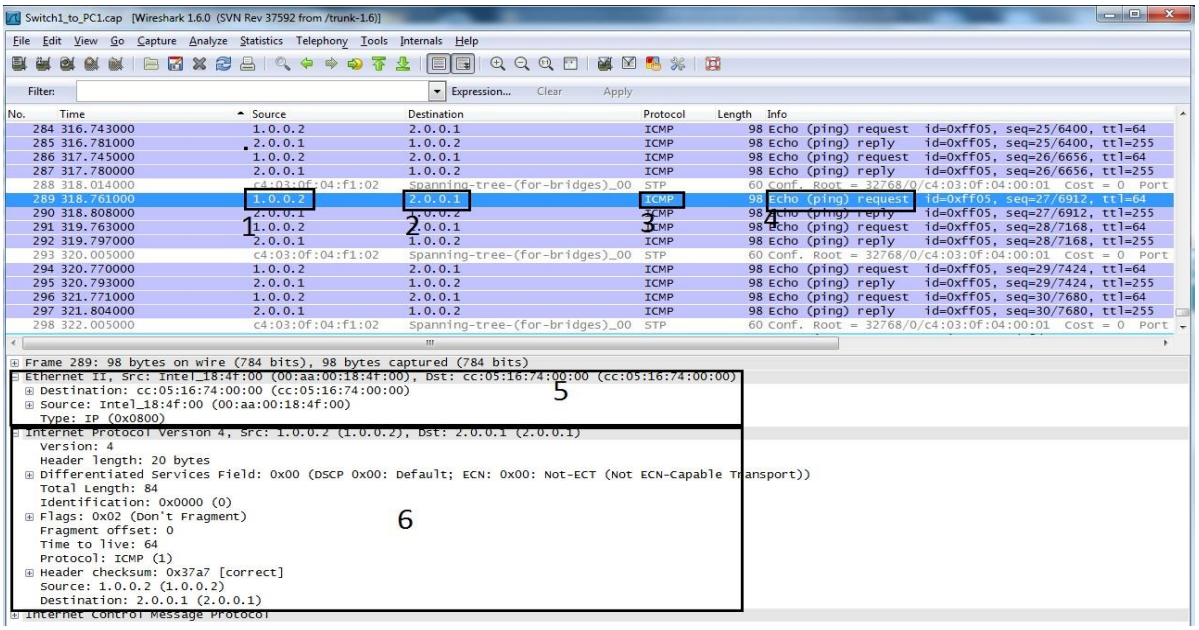

Рисунок 7 – Пример захвата пакета ICMP echo request

Пакет отправленный с компьютера PC1 до PC2, пройдет следующий маршрут:

PC1(int e0) =1=> (int f1/2)Switch1(int f1/0) =2=> (int f1/0)Switch2 (int f1/2)=3=> (int f0/0.2) Router (int f0/0.3) =4=> (int f1/2)Switch2 (int f1/0) =5=> (int f1/0)Switch1(int f1/2) =6=> (int e0)PC2

ЗАДАНИЕ

1. Составьте исходную топологии;
2. Получите листинг команд конфигурации, либо конфигурационные файлы;
3. Сделайте захваты следующих пакетов с помощью программы Wireshark: Arp request, Arp reply, ICMP echo request, ICMP echo reply, поясните значение всех полей данных пакетов.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Формат метки VLAN согласно стандарту IEEE802.1 q;
2. Объясните принцип коммутации пакетов с учетом техники VLAN;
3. Дайте определение виртуальной локальной сети;
4. В чем разница между транкинговым портом и портом магистральным;
5. Какое максимальное количество VLAN можно организовать согласно стандарту IEEE 802.1q;
6. Поясните процедуру передачи пакета ICMP echo request от PC1 к PC2.

СПИСОК ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы:Учебник для вузов [Текст]/ В.Г. Олифер, Н.А. Олифер, 4-е изд.: СПб.: Питер, 2006 -958 с.
2. Сергеев А.Н. Основы локальных компьютерных сетей [Текст]/ Сергеев А.Н.: Изд.: «Лань», 2016. 184 с.
3. Электронный каталог Documentation [Электронный ресурс]: / Internet. - http://www.gns3.net/documentation/ (10.10.17).